Formal Proofs of Inequalities and Semi-Definite Programming

Supervisor: Benjamin Werner (TypiCal)
Co-Supervisor: Stéphane Gaubert (Maxplus)

2^{nd} year PhD Victor MAGRON

LIX, École Polytechnique

Friday November 27 th 2011

Contents

- Background
- Difficulties
- Sums of Squares (SOS) and Semi-Definite Programming (SDP) Relaxations
- Formal Proofs of Non-linear Inequalities
  1. Certificates and Oracles
  2. Flyspeck
  3. Bernstein
  4. SOS and Transcendental Functions
  5. Possible Framework

Background

- Computational Proofs: Primality, Four colors theorem
- Autarcic approach: a program **prime** : `nat` $\longrightarrow$ `bool` computes prime numbers with an algorithm proved sound and correct in Coq, no need of certificates to check the primality
- Sceptic approach: a program **prime** : `nat` $*$ `cert` $\longrightarrow$ `bool` in Coq checks primality, helped with the certificate imported from an external tool
- Hales proof of the Kepler conjecture generated hundred of non-linear inequalities: need automatic proofs

Difficulties

- Multiple interests:
  - A part of the mathematics is related to these technics
  - The interface between the deductive « conventional » part and the computational part is particularly favorable to errors
  - Opening new fields to proof systems while allowing some results automatization
- Improve the tools developed by Roland Zumkeller by using SDP tools (strong interest for the related applied mathematics)
- Limit the size of the certificate while using hybrid format for numbers, mixing classical numerical and symbolic representation

SOS and SDP Relaxations

- Polynomial Optimization Problem (POP):

  Let $f_k \in \mathbb{R}[\mathbf{x}]$ $(k = 0, 1, \dots, m)$:

  minimize $f_0(\mathbf{x})$ subject to $f_k(\mathbf{x}) \geqslant 0$ $(k = 1, 2 \dots, m)$

- Generalized Lagrangian dual:

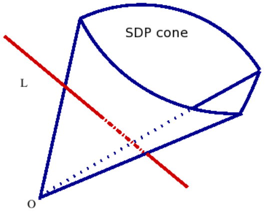
  $L(\mathbf{x}, \boldsymbol{\varphi}) = f_0(\mathbf{x}) - \sum_{k=1}^{m} \varphi_k(\mathbf{x}) f_k(\mathbf{x})$ $(\forall \mathbf{x} \in \mathbb{R}^n$ and $\forall \boldsymbol{\varphi} \in \Phi)$,

  $\Phi = \{\boldsymbol{\varphi} = (\varphi_1, \varphi_2, \dots, \varphi_m) : \forall k \in \{1, 2 \dots, m\}, \ \varphi_k$ SOS$\}$

- Lagrangian relaxation problem:

  $$\left.\begin{array}{l} L^*(\boldsymbol{\varphi}) = \inf\{L(\mathbf{x}, \varphi) : \mathbf{x} \in \mathbb{R}^n\} \\ \zeta^* = \inf\{f_0(\mathbf{x}) : f_k(\mathbf{x}) \geqslant 0 \ (k = 1, 2 \dots, m)\} \end{array}\right\} L^*(\boldsymbol{\varphi}) \leqslant \zeta^*$$

- Constrained optimization problems with semi-definite positive matrices:



Find $X \in \mathbb{S}^n$, solution of the primal problem:

$$
(P) \begin{cases} \inf \langle C, X \rangle \\ A(X) = b \\ X \succeq 0. \end{cases}
$$

- Such formulations can be derived from the previous problem as primal SDP relaxations.

Formal Proofs of Non-linear Inequalities - Certificates and Oracles

- Proof systems like Coq have several ways to solve such problems:
  1. Without certificates, with pure functional computations (OCaml fragment) : **autarcic** approach (Bernstein, TM)
  2. Coq checks certificates imported from external solvers (e.g. Gloptipoly, SparsePOP, RAGlib, CSDP,...): **sceptical** approach with formal computations
- Micromega: `psatz` tactic in Coq, developed by F. Besson, uses sceptical approach by verification of certificates imported from CSDP computations
- Such tactics can be developed with several computational tools: Bernstein, SOS, rational functions minimization, transcendental approximations,...

- Two types of inequalities issued from Flyspeck non-linear part:
  1. Pure polynomials
  2. Transcendentals
- Example: dih $x = \dfrac{\pi}{2} + \arctan \dfrac{-\partial_4 \Delta x}{\sqrt{4 x_1 \Delta x}}$

  $K = ([4; 6.3504]^3, [6.3504; 6.3504], [4; 6.3504]^2)$

$$\Delta x = \frac{1}{2} \begin{vmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & x_3 & x_2 & x_1 \\ 1 & x_3 & 0 & x_4 & x_5 \\ 1 & x_2 & x_4 & 0 & x_6 \\ 1 & x_1 & x_5 & x_6 & 0 \end{vmatrix} = \begin{array}{l} x_1 x_4 (-x_1 + x_2 + x_3 - x_4 + x_5 + x_6) \\ + x_2 x_5 (x_1 - x_2 + x_3 + x_4 - x_5 + x_6) \\ + x_3 x_6 (x_1 + x_2 - x_3 + x_4 + x_5 - x_6) \\ - x_2 x_3 x_4 - x_1 x_3 x_5 - x_1 x_2 x_6 - x_4 x_5 x_6 \end{array}$$

Lemma$_{2570626711}$: $\forall x \in K$, dih $x \geqslant 1.15$.

Formal Proofs of Non-linear Inequalities - Bernstein

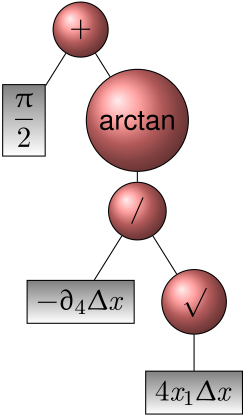
- PhD thesis of Roland Zumkeller about Bernstein polynomials and Taylor models (TM): Global Optimization in Type Theory
- Software: `sergei` written in Haskell can provide bounds for multivariate polynomials
- Sufficent for the former example:
  $\forall x \in ([4; 6.3504]^3, [6.3504; 6.3504], [4; 6.3504]^2)$,
  max $((\partial_4 \Delta x)^2 - 0.2(4 x_1 \Delta x)) < 0$ and
  dih $x =$ arctan$(-\sqrt{0.2}) + \dfrac{\pi}{2} > 1.1502 > 1.15$
- Work in progress: a formal study of Bernstein coefficients and polynomials by Bertot, Guilhot and Mahboubi

Formal Proofs of Non-linear Inequalities - SOS and Transcendental Functions

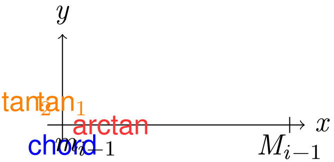
- Need to deal with rational functions minimization or constrained POP: Taylor Models in Coq, Gloptipoly, SparsePOP, RAGlib
- Gloptipoly or RAGlib can solve the former example
- Not sufficent to solve many inequalities, e.g. with sums or multiplications of transcendental functions

Formal Proofs of Non-linear Inequalities - Possible Framework

- Build abstract syntax tree from an inequality, where leaves are polynomials and nodes are transcendental functions (arctan, $\sqrt{}$, ...) or basic operations ($+$, $*$, $-$, $/$), e.g. :

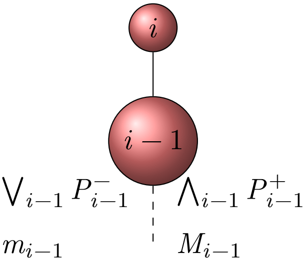


- Use basic convexity properties and monotonicity of elementary functions to find **lower** and **upper** piecewise polynomial bounds for each **node**, e.g.:



Formal Proofs of Non-linear Inequalities - Possible Framework

- Recursive algorithm solving successive constrained POP at unary or binary nodes i, e.g.:



- $\bigvee_{i,k} \text{tan}_k(P^-_{i-1}(x)) = P^-_i$
- $\bigwedge_i \text{chord}(P^+_{i-1}(x)) = P^+_i$

$$\begin{cases} \min z = m_i \\ z \geqslant P^-_i(x) \\ x \in K \end{cases} \quad \begin{cases} \max z = M_i \\ z \leqslant P^+_i(x) \\ x \in K \end{cases}$$

- Works out sometimes with a single tangent at each node and `sergei` but fails with several tangents and SOS solvers

Formal Proofs of Non-linear Inequalities - Possible Framework

- For the binary node of addition:

$$\begin{cases} \text{min } z \\ z \geqslant z_1 + z_2 \\ z_1 \geqslant \bigvee_k P_k^- \\ z_2 \geqslant \bigvee_l P_l^- \end{cases} \begin{cases} \text{max } z \\ z \leqslant z_1 + z_2 \\ z_1 \leqslant \bigwedge_k P_k^+ \\ z_2 \leqslant \bigwedge_l P_l^+ \end{cases}$$

End

Thank you for your attention!